AMENDMENTS TO THE SPECIFICATION

Please amend the title to read:

a1

METHOD FOR REPEATED AUTHENTICATION OF A USER SUBSCRIPTION IDENTITY MODULE

Please insert the following replacement paragraph in place of the paragraph beginning at line 28 on page 5 of the specification:

For ease of explanation only, the AKA procedure will now be described in the context of a communication system part of which is shown in FIG. 1. The communication system shown in FIG. 1 complies with the 3GPP TSG33.102 standard. Initially, the AV is transferred from HLR 100 to the VLR at base station 104 (or to a VLR coupled to base station 104). In accordance with the standard, the VLR derives XRES from the received AV. The VLR also derives AUTN and RAND from the received AV and transfers them to mobile 108 via communication link 106. Mobile 108 receives AUTN and RAND and transfers the RAND and AUTN to its USIM. The

a2

USIM validates the received AUTN as follows: The USIM uses the stored secret key (K_i) and RAND to compute the AK, and then uncovers the SQN. The USIM uncovers the SQN by exclusive OR-ing the received AK $\oplus$ SQN with the computed value of AK_i; the result is the uncovered or deciphered SQN. Then the USIM computes the MAC and compares it to the MAC received as a part of the AUTN. If MAC checks, (*i.e.* received MAC = computed MAC) the USIM verifies that the SQN is in a valid acceptable range (as defined by the standard), in which case the USIM considers this attempt at authentication to be a valid one. The USIM uses the stored secret key (K_i) and RAND to compute RES, CK and IK. The RES is a Mobile Station Response. The USIM then transfers IK, CK and RES to the mobile shell and causes the mobile

to transmit (via communication link 106) RES to base station 104. RES is received by base station 104 which transfers it to the VLR. The VLR compares RES to XRES and if they are equal to each other, the VLR also derives the CK and IK keys from the Authentication Vector. Because of the equality of XRES to RES, the keys computed by the mobile are equal to the keys computed by the HLR and delivered to the VLR.